UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,403	07/26/2001	William Michael Raike	SMD-002	4247

51414 7590 07/31/2006

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
EXCHANGE PLACE
BOSTON, MA 02109-2881

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 07/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/912,403	RAIKE, WILLIAM MICHAEL	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims 2-5, 9 ~ 11-16

4)☒ Claim(s) ~~1-16~~ is/are pending in the application.

4a) Of the above claim(s) ~~1, 6-8 and 10~~ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-5, 9, 11-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to the communication dated May 25, 2006 with the amendments to claims 4-5, 9,11, 13 and 15-16 and the cancellation of claims 1 and 6-8 and 10.

2. Claims 2-5, 9 and 11-16 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 2-5, 9 and 11-16 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

4. Claim 12 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 12 does not appear to further limit claim 3 because it defines public key encryption algorithm is asymmetric. If it limits claim 3, it should state public encryption is RSA, El-Gamal, etc. Applicant needs to either cancel claim 12 or clearly explain asymmetric.

5. Claim 2 depends on the cancelled claim 10. Appropriate correction is required.

6. Claim 5 is objected to because of the following informalities: “the a” should be "a". Appropriate correction is required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 3-5, 9 and 11-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski (5,420,866) in view of Bleichenbacher et al. (6,735,313) in view of Levy et al (6,212,633) and further in view of Warren et al. (5,963,909).

a) As to claims 9, 11, 13 and 15, Wasilewski discloses methods for providing conditional access information to decoders in a packet-based multiplexed communications system comprising a transmitter (Fig. 2, element 198) encrypts payload sections of each transport packet stream of data (col. 9, lines 30-36) that assigned a unique packet ID (PID) (col. 8, lines 44-46) using unique encryption control words (col. 9, lines 26-30); transmitter adds the packet ID to the corresponding encrypted packet data; inserts the packet so processed into the packet stream and transmit the encrypted data packet stream, unique packet ID and the packet key to the recipient (Figs. 3A and 3B; col. 9, lines 45-47). Wasilewski also discloses at the recipient's station (Fig. 2, element 201), each received encrypted packet is decrypted by the decryption information respective to each packet ID (Fig. 6; col. 14, lines 13-20) and the decrypted packet data is outputted in a form suitable for playing the streamed media (Fig. 2, element 208).

Wasilewski does not specifically disclose the encryption key (i.e. packet key) used for encrypting packet data is being based on the random base key and the assigned tag value of the packet.

Bleichenbacher discloses a system for transmitting an encrypted program together with a program identifier which is used by a set top terminal, together with stored entitlement information, to derive the decryption key necessary to decrypt the program (col. 1, lines 9-15), the system comprising a program key used to encrypt each program (col. 3, lines 4-6), the program key is created by applying a hash function to the master key and program identifier (col. 3, lines 30-37). The master key which reads on the base key may be updated for security reason (col. 7, lines 21-23). Bleichenbacher also discloses the decryption process (Fig. 9).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of creating a packet key based on a base key and a unique packet tag assigned to each data packet in the system of Wasilewski as Bleichenbacher discloses so as to enhance security of key and data against hackers.

Wasilewski and Bleichenbacher do not explicitly disclose encrypting the streaming media by creating different packet keys for each data packet of the streaming media and encrypting each data packet using the corresponding packet keys.

Warren is relied on for the teaching of encrypting the streaming media by creating different packet keys for each data packet of the streaming media and encrypting each data packet using the corresponding packet keys (Fig. 12).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of encrypting the streaming media by creating different packet keys for each data packet of the streaming media and encrypting each data packet using the corresponding packet keys in the system of Wasilewski and Bleichenbacher as Warren discloses so as to enhance security of key and data against hackers.

Wasilewski, Bleichenbacher and Warren do not explicitly disclose encrypting the base key, thus creating an open key.

Levy is relied on for the teaching of generating randomly a session key, encrypting the session key (col. 13, line 64 to col. 14, line 3) and transmit the encrypted session key to target node (col. 14, lines 15-17).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of encrypting the base key using a public key encryption algorithm as Levy teaches in the system of Wasilewski, Bleichenbacher and Warren so as to enhance the security of transmitted information.

b) As to claims 3, 12 and 14, please see addressed claim 9 above.

c) As to claim 4, Wasilewski, as modified above, discloses the packet data is encrypted using a symmetric encryption algorithm in conjunction with the packet key and the encrypted data is decrypted at the recipient's station using the symmetric encryption algorithm in conjunction with the recreated packet key (col. 3, line 45 to col. 4, line 6).

d) As to claims 5 and 16, Bleichenbacher, as modified above, discloses the hash function used to create and reestablish the packet key is SHA-1 or MD5 (col. 5, lines 43-47).

9. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski (5,420,866) in view of Bleichenbacher et al. (6,735,313) in view of Levy et al (6,212,633) in view of Warren et al. (5,963,909).and further in view of Hawthorne (5,768,381).

Wasilewski, Bleichenbacher, Levy and Warren do not specifically disclose transmitting the open key by adding it to a header of the transmission.

Hawthorne discloses encryption and decryption of electronically transmitted messages (col. 1, lines 6-10) comprising transmitting encrypted session key (i.e. open key) as header to the recipient.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of transmitting the open key to the recipient by adding it to the stream header in the system of Wasilewski, Bleichenbacher, Levy and Warren as Hawthorne teaches so as to strengthen secure communications between two entities.

Conclusion

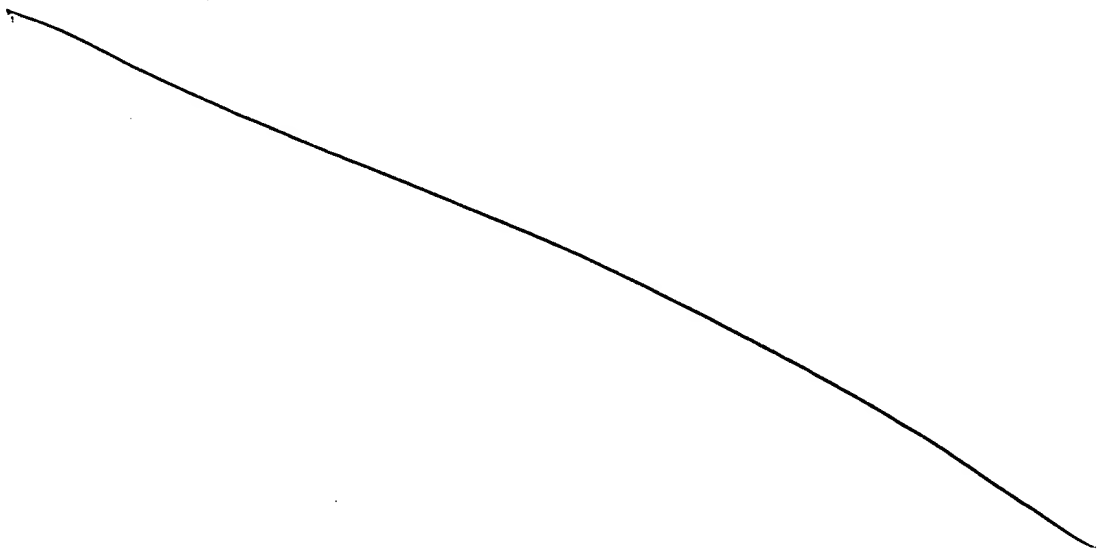
Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.



Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

mdn
7/25/06

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100